A Secure Cooperative Sensing Protocol for Cognitive Radio Networks

Carles Garrigues
Estudios de Informática, Multimedia y Telecomunicación
Universitat Oberta de Catalunya
Email: cgarrigueso@uoc.edu

Helena Rifà-Pous
Estudios de Informática, Multimedia y Telecomunicación
Universitat Oberta de Catalunya
Email: hrifa@uoc.edu

***Abstract*—Cognitive radio networks sense spectrum occupancy and manage themselves to operate in unused bands without disturbing licensed users. Spectrum sensing is more accurate if jointly performed by several reliable nodes. Even though cooperative sensing is an active area of research, the secure authentication of local sensing reports remains unsolved, thus empowering false results. This paper presents a distributed protocol based on digital signatures and hash functions, and an analysis of its security features. The system allows determining a final sensing decision from multiple sources in a quick and secure way.**

***Index Terms*—authentication, cognitive radio, cooperative sensing, cryptography**

I. Introduction

Spectrum is an essential resource for the provision of mobile services. In order to control and delimit its use, governmental agencies set up regulatory policies. Unfortunately, such policies have led to a deficiency of spectrum as only few frequency bands are left unlicensed, and these are used for the majority of new emerging wireless applications. Besides, studies conducted by the Spectrum Policy Task Force show that most of the licensed spectrum is largely under-utilized [1].

One promising way to alleviate the spectrum shortage problem is adopting a spectrum sharing paradigm in which frequency bands are used opportunistically. In this scheme, those who own the license to use the spectrum are referred to as primary users, and those who access the spectrum opportunistically are referred to as secondary users. Secondary users must not interfere with primary ones, who always have usage priority.

The enabling technology for opportunistic sharing is cognitive radio (CR) [2]. A CR is a system that senses its electromagnetic environment and can dynamically and autonomously adjust its operating parameters to access the spectrum. CR terminals form self-organizing networks capable to detect vacant spectrum bands that can be used without harmful interference with primary users. Once a vacant band is found, secondary users coordinate themselves in order to share the available spectrum.

Performing reliable spectrum sensing is a difficult task. Wireless channels can suffer fading, thus provoking the hidden node problem in which a secondary user fails to detect a primary transmitter. The most important challenge for a CR is to identify the presence of primary users, and, for this reason, secondary users must be significantly more sensitive in detecting primary transmissions than primary receivers.

In order to reduce the sensitivity requirements of individual CRs, recent studies propose performing distributed spectrum sensing (DSS)[3]. In DSS, multiple secondary users cooperate and share their local sensing results, which are then merged together to reach a final decision. Although the use of cooperation in spectrum sensing has been extensively studied, some security issues still remain unsolved.

The problem of current spectrum sensing protocols is that they do not provide any mechanism to authenticate the observations exchanged by secondary users. This problem is present even in those protocols that intend to deal with malicious users. Secure spectrum sensing protocols assume that sensing reports from secondary users can be effectively authenticated. As a result, malicious users can be detected - their reports repeatedly differ from the final decision- and their contributions discarded. However, a mechanism to authenticate the observations sent by secondary users is still missing.

This paper presents a protocol that enables the secure authentication of sensing information. The protocol is mainly based on the use of hash functions, so that authentication is carried out as quickly as possible. Performing spectrum sensing without significant delay is essential because a lengthy sensing process reduces the time left for transmission. Furthermore, a lengthy sensing process will certainly consume more energy at the CR. Thus, the combination of the proposed protocol with the existing data fusion schemes allows distributed spectrum sensing to be conducted effectively.

II. Background

Cooperative sensing is based on merging the local observations of multiple secondary users. Traditionally, there are two techniques which are used for local spectrum sensing: energy detection or cyclostationary feature detection. Energy detection is based on integrating the energy received over an observation interval. This method is optimal when secondary users do not have sufficient information about the primary user signal. On the other hand, cyclostationary feature detection takes advantage of the fact that signals used in wireless communications are cyclostationary. Thus, their features can

be detected using a spectral correlation function. However this method requires longer observation times.

Since local spectrum sensing results are subject to multi-path and/or shadowing fading, the cooperation among CRs is fundamental to achieve a reliable decision. This cooperation can be implemented in a centralized or distributed manner. In the centralized method, the base station or fusion center (FC) gathers all the information from secondary users and executes the data fusion to reach the final decision. On the other hand, distributed solutions require all secondary users to exchange their local observations, so that the data fusion operation is carried out independently on each secondary device.

Several data fusion schemes have been proposed to merge the sensing data observed by each secondary user. These schemes are based on exchanging of more or less information depending on whether devices perform hard or soft cooperation. When hard cooperation is employed, radios only exchange their final decision: primary user detected or not detected. On the other hand, soft cooperation means that radios exchange their local test statistics with each other. Among the proposed methods, the most typical one is based on applying the "k out of N" rule. This rule determines that the channel is occupied if at least k of the N secondary users have detected the primary signal. As avoiding interference with primary users is a top priority, the most common value of k is 1.

Other methods proposed for merging the sensing data are based on modeling the fusion process as a probabilistic problem. Zarrin and Lim [4] compute the probability of detection by performing the likelihood ratio test (LRT), which is based on the Neyman-Pearson theorem and is used for optimal decision making. Wang et al. [5] apply another probabilistic method where secondary users are classified according to their SNR level and those with higher levels are given more influence on the final decision. Alternatively, Chen et al. [6] propose the use of a Sequential Probability Ratio Test (SPRT). SPRT is a data fusion scheme that supports a variable number of local spectrum sensing results. The protocol assumes that the number of sensing results can be increased and adjusted as necessary, so it guarantees both a bounded false alarm probability and a bounded miss detection probability. The authors also suggest the use of a reputation-based scheme to increase the robustness of the data fusion process.

The introduction of reputation mechanisms in the sensing process has also been considered in some studies. In [7], a two-step protocol for the detection of malicious users that report false sensing data is proposed. In the first step, an outlier detection method is applied to pre-filter those sensing results that are too distant from the rest of the data. In the second step, each user is associated with a trust factor that is based on the past and present sensing data sent by the user. Thus, the trust factor lends more or less weight to a decision depending on the reliability of the corresponding user.

Another important issue to take into account when performing spectrum sensing is preventing primary user emulation attacks. These attacks allow a malicious secondary user to gain priority over others by emulating the signal of a primary user. Solutions to this problem are based on checking whether the estimated location of the transmitter and its signal characteristics match the ones of the licensed primary user [8].

As we have shown, several studies have approached the problem of providing security and reliability to the spectrum sensing process. However, no proposal has been presented so far to authenticate the sensing data provided by a secondary user. Without such authentication, the proposals based on associating a reputation or a probability of detection to each user become useless. The combination of existing protocols with a secure authentication method can undoubtedly improve the performance of spectrum sensing protocols in the presence of faulty radios or malicious users.

III. Protocol

This section presents our protocol for the secure authentication of users' sensing reports. The protocol prevents users from illegitimately claiming false identities and from injecting fake sensing data. Thus, the protocol aims at withstanding the following attacks:

- Altering the final sensing decision. A user could increment her weight in the data fusion process by forging several identities and making a contribution for each of them. With enough forged identities, a user might be able to completely alter the aggregate reading.
- Deceiving the reputation system. By using a different identity each time, a user might report false sensing data repeatedly and avoid earning a bad reputation.
- Obtaining resources unfairly. A user could use many identities to obtain more than her fair share of resources (e.g. bandwidth).

The proposed protocol assumes that the cooperation among CR's is implemented in a centralized manner, which is the most frequently used configuration in the spectrum sensing protocols presented to date. We also assume that the secondary users and the fusion center can use a common control channel.

To perform distributed sensing securely, the cooperative system should identify the users that participate in the sensing process, authenticate their claims, and weigh up their contribution to the final decision based on their reputation or probability of successful detection. Our protocol focuses on the mechanisms required to identify the users and authenticate their sensing results. The final part of the distributed sensing process (i.e. weighing up and merging the contributions) can be implemented using any of the mechanisms that we have mentioned in the previous section. The selection of which data fusion technique to use is out of the scope of this paper.

One of the key goals of the protocol design has been to develop a quick authentication process. We take a public key infrastructure (PKI) approach to identify the peers of the network through digital signatures. Even though this process is costly, it has to be executed only once, in the setup phase. Then, we make use of efficient Hash Message Authentication Code (HMAC) functions to protect users' sensing reports from forgery and manipulation.

HMAC functions provide message authenticity and integrity by calculating a hash of two inputs: the target message and a secret key. In our protocol, we use hash chains to produce one time secret keys. Hash Chains, first proposed by Lamport [9], are versatile low-cost constructions that are used extensively in various cryptographic systems.

The proposed protocol is divided in two phases. The first phase is the identification of users, and the second one is the collection of sensing results. In the following sections, we will describe each one of these phases in detail.

A. Phase 1: user authentication

In the first phase, the user contacts the fusion center (which can be, for instance, the base station) and asks permission to join the cognitive radio network. Besides, she commits to a hash chain by attaching the top value of the chain in the request. This process requires mutual authentication using digital signatures. At this point, the fusion center decides whether or not to accept the user into the network. The following are the detailed steps carried out during this phase.

1) User U chooses a random number w_N and prepares a hash chain of length N, where N is chosen by the fusion center and it is shared by all network members.
   Hash chains are composed of a sequence of values that can only be computed in one-way. A hash chain of length N is constructed by applying a one-way hash function H(.) recursively to an initial seed value w_N: $w_{N-1} = H(w_N)$, $w_{N-2} = H(w_{N-1})$, $\cdots$, $w_0 = H^N(w_N)$. In general, $w_i = H(w_{i+1}) = H^{N-i}(w_N)$.
2) U sends the top value of her chain (w_0) to the fusion center FC in a digitally signed message. The signature is computed using U's private key pvk_U. She also includes information about her identity Id_U (i.e. the unique identifier of her public key certificate).

$$JoinReq = \{w_0, Id_U, Sign_{pvk_U}(w_0, Id_U)\}$$

3) FC verifies the signature received from U using U's public key pbk_U. If the signature is correct, FC decides whether or not to accept U into the network. This decision will be based, for example, on the reputation earned by U in previous processes. The implementation of these mechanisms is out of the scope of this paper.

B. Phase 2: collection of local sensing results

In the second phase, the fusion center requests each user to sense a certain set of frequency bands. Users conduct spectrum sensing using a mechanism based on the energy perceived, cyclostationary statistics, or any other method. Then, they sign their own local sensing results with a HMAC function and send the sensing data and its signature to the fusion center. The keys used to compute the HMACs are taken from the hash chain, so that the fusion center can verify the identity of the sender. The following are the detailed steps carried out in this phase.

1) At time t, FC broadcasts a signed message with a task list ($TaskList$) that contains the list of channels each user has to sense.

$$SensingReq_t = TaskList_t, Sign_{pvk_B}(TaskList_t, t)$$

where

$$TaskList_t = [(Id_0, ChannelList_0, i_0) \cdots (Id_S, ChannelList_S, i_S)]$$

In the above expression, S is the total number of secondary users, and i_j is the hash chain index that points to the value the user j must use in the following step.

2) Each user U verifies the signature of the sensing request and, if correct, senses the channels listed in $ChannelList_U$. After completing the sensing process, each user sends the results $SensingRes$ to FC. These results can be binary decisions or long test statistics, depending on whether hard or soft cooperation is in use. To allow the authentication of the sensing results, these are sent as follows:

$$SignRes_t = SensingRes_t, HMAC(SensingRes_t, w_i)$$

The key used to construct the HMAC is w_i, where i is the index received from FC in $SensingReq_t$.

3) FC waits for the reply of all secondary users and at time t' (with $t' = t + \Delta t$), it generates a new $TaskList_{t'}$. This new task list can contain empty $ChannelLists$ if there are not more channels to sense.

$$SensingReq_{t'} = TaskList_{t'}, Sign_{pvk_B}(TaskList_{t'})$$

where

$$TaskList_{t'} = [(Id_0, ChannelList_0, \{i+1\}_0) \cdots (Id_S, ChannelList_S, \{i+1\}_S)]$$

4) Each user U verifies the signature of the sensing request and creates a reply that depends on whether the corresponding $ChannelList$ is empty or not. If $ChannelList$ is not empty, then the results are constructed as follows:

$$SignRes_{t'} = SensingRes_{t'}, HMAC(SensingRes_{t'}, w_{i+1}), w_i$$

Otherwise, they just contain the key needed to verify the previous HMAC sent to FC in $SignRes_t$.

$$SignRes_{t'} = w_i$$

As can be seen, the response always includes the key w_i used to create the previous signed results sent in $SignRes_t$.

5) FC waits for the reply of all secondary users and verifies the HMACs from the $SignReq_t$. If more channels need to be sensed or more HMACs need to be verified, a new request is generated. Otherwise, FC starts the fusion of the sensing results.

IV. Discussion

The presented protocol provides a way to authenticate sensing reports with a minimum overhead. Each user has to generate a digital signature when she accesses the fusion center for the first time. Afterwards, she only has to validate digital signatures (which is very efficient [10]), and compute HMAC using a costless hash function. The HMAC keys can be generated and checked with efficient mechanisms for fast chain traversal [11], [12] and for economic setup and verification [13], [14]: a one-way chain with N elements only requires log(N) storage and log(N) computation to access an element.

From the security point of view, the proposed system is robust against Sybil attacks, in which a user illegitimately claims multiple identities, and the injection of false sensing reports. Sybil attacks are prevented using certificates generated by a trusted central authority. If a user does not own a valid certificate, she is not authorized in the CR network and can not send sensing reports to the fusion center. On the other hand, the injection of false sensing reports is avoided using verifiable HMAC signed reports.

Reporting a verifiable sensing result involves two user transmissions. First, the user sends the sensing data and its corresponding HMAC. Then, she reveals the HMAC key, which is an element of a hash chain. The fusion center verifies the integrity of the sensing message and the authenticity of the key.

Sensing reports are protected against modification attacks since they are signed with an HMAC. Keys used to compute the HMAC are taken from the secret hash chain w of each user. Therefore, only the user who created the hash chain can compute the corresponding HMAC.

Reply attacks are avoided because each HMAC key is used only once. The fusion center indicates in the sensing request which element i it has to be used. Chain elements are asked in ascending order (w_0, w_1, .. w_N) so knowing a user's previous key gives no information about the present one. Moreover, the sensing request is signed so that an attacker can not modify the requested hash index.

Additionally, as the sensing requests and replies are synchronized by i, it is not effective to block the user's reports in order to steal her keys to later generate fake reports.

V. Conclusion

In this paper, we have identified the security vulnerabilities of a cooperative sensing process and its prejudicial effects in CR networks. We have proposed a secure protocol for centralized based systems that uses digital signatures and hash functions.

The protocol enables the fusion center to verify the identity of network members and to ensure the received sensing information is really originated from the claimed source. One of the main features of the proposal is the fact that is computationally efficient and introduces a small bandwidth overhead. As part of our future research, we plan to integrate reputation measures into the scheme.

Acknowledgements

This work is partially supported by the Spanish Ministry of Science and Innovation and the FEDER funds under the grants TSI-020100-2009-374 SAT2, TSI2007-65406-C03-03 E-AEGIS and CONSOLIDER CSD2007-00004 ARES.

References

[1] Federal Communications Commission. Spectrum policy task force report. ET Docket No. 02-135. Technical report, 2002.

[2] J. Mitola III and G.Q. Maguire Jr. Cognitive radio: making software radios more personal. *IEEE personal communications*, 6(4):13–18, 1999.

[3] S.M. Mishra, A. Sahai, and R.W. Brodersen. Cooperative sensing among cognitive radios. In *IEEE International Conference on Communications*, pages 1658–1663. IEEE Computer Society, 2006.

[4] S. Zarrin and T.J. Lim. Belief Propagation on Factor Graphs for Cooperative Spectrum Sensing in Cognitive Radio. In *IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN)*, pages 1–9. IEEE Computer Society, 2008.

[5] W. Wang, W. Zou, Z. Zhou, and Y. Ye. Detection Fusion by Hierarchy Rule for Cognitive Radio. In *Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom)*, pages 1–5. IEEE Computer Society, 2008.

[6] Ruiliang Chen, Jung-Min Park, Y.T. Hou, and J.H. Reed. Toward secure distributed spectrum sensing in cognitive radio networks. *Communications Magazine, IEEE*, 46(4):50–55, April 2008.

[7] P. Kaligineedi, M. Khabbazian, and V.K. Bhargava. Secure cooperative sensing techniques for cognitive radio systems. In *IEEE International Conference on Communications (ICC)*, pages 3406–3410, May 2008.

[8] R. Chen, J.M. Park, and J.H. Reed. Defense against primary user emulation attacks in cognitive radio networks. *IEEE Journal on Selected Areas in Communications*, 26(1):25–37, 2008.

[9] Leslie Lamport. Password authentication with insecure communication. *Commun. ACM*, 24(11):770–772, 1981.

[10] Helena Rifà-Pous and Jordi Herrera-Joancomartí. Cryptographic energy costs are assumable in ad hoc networks. *IEICE Transactions on Information and Systems*, E92.D(5):1194–1196, 2009.

[11] Don Coppersmith and Markus Jakobsson. Almost optimal hash sequence traversal. In *Financial Cryptography*, volume 2357 of *LNCS*, pages 102–119, 2002.

[12] Yaron Sella. On the computation-storage trade-offs of hash chain traversal. In *Financial Cryptography*, volume 2742 of *LNCS*, pages 270–285, 2003.

[13] Markus Jakobsson, Frank Thomson Leighton, Silvio Micali, and Michael Szydlo. Fractal merkle tree representation and traversal. In *The Cryptographers' Track at the RSA Conference (CT-RSA)*, volume 2612 of *LNCS*, pages 314–326, 2003.

[14] Marc Fischlin. Fast verification of hash chains. In *The Cryptographers' Track at the RSA Conference (CT-RSA)*, volume 2964 of *LNCS*, pages 339–352, 2004.